Securing Public Applications with SonicWall Cloud Secure Edge (CSE)

Protect SaaS applications via CSE's Cloud Access Security Broker (CASB) solution

Updated on 5 minutes to read Contributors  

Overview

Public applications, also known as **Software-as-a-Service (SaaS) applications**, are cloud-based software hosted and delivered by software vendors. Because these applications are public resources hosted on your vendor's servers and accessed over the internet (unlike private resources which are hosted on your servers in your private networks) they often bypass key enterprise security controls.

Most organizations enable Single Sign On (SSO) and Multi-factor Authentication (MFA) for strong user authentication to public applications, but are unable to enforce zero-trust security controls such as device trust requirements for device posture validation, continuous authorization to revoke user access mid-session, etc.

Enforcing zero-trust security for SaaS applications is particularly challenging because of the variety of applications an organization uses and the different levels of risk they pose. Furthermore, a one-size-fits-all approach to zero-trust security seldom works because SaaS applications are central to myriad critical workflows, such as access from native apps, access from employee-owned mobile devices, third-party access from unmanaged devices, cloud-based integrations with other products, etc.

CSE offers two techniques to provide zero-trust security for public applications - **IP Allowlisting** and **Authentication Federation**. Both techniques are designed to provide seamless access to users and devices while enforcing security controls the enterprise need. Both techniques can be applied at your Identity Provider or at the SaaS Application itself, and leverage CSE's trust scoring and access policy frameworks. Most organizations utilize both techniques in concert to secure their public applications.

Technique	Service Type	Description
IP Allowlisting	Service Tunnel	Configure network access rules with IP ranges that are allowed to connect
Authentication Federation	Federated SaaS App	Configure authentication flow to federate to CSE to validate device trust

Use Cases

You may use just one or both techniques to secure public applications used by your organization. Some common scenarios for each technique are listed below, along with the request flow diagram that describes how the zero-trust security mechanism works.

IP Allowlisted SaaS Applications

You can define a Service Tunnel in CSE and configure IP allowlisting when you need to enable:

- Restricted access to public applications that are *not* integrated with your IDP
- Device trust for a specific SaaS application(s) without changing authentication settings in IDP or the application
- A migration of IP allowlisting from the corporate VPN to a modern VPNaaS

Federated SaaS Applications

You can define a Federated SaaS App in CSE and configure authentication federation when you need to enable:

- Device trust checks without running a VPN client or intercept network traffic on the device
- Device trust checks and certificate authentication before users can establish a single sign-on session with your IDP
- Device trust checks and certificate authentication before users can access SaaS applications integrated with your IDP
- SAML/OIDC authentication and device trust policy enforcement for custom SaaS applications

FAQs

Do you provide a Proxy-based CASB?

Do you provide an API-based CASB?

What's next

Read about how to configure IP Allowlisting and Authentication Federation in CSE.

SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

- Concepts
- Components
- Release Notes

Guides

- Quick Start Guides
- Solutions
- Feature Guides
- API Guide